Chapter 3

Quantum Flows for Secret Key Distribution

Luis A. Lizama-Pérez, J. Mauricio López and
Eduardo de Carlos Lopez

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75964

Abstract

Despite the unconditionally secure theory of quantum key distribution (QKD), several attacks have been successfully implemented against commercial QKD systems. Those systems have exhibited some flaws, as the secret key rate of corresponding protocols remains unaltered, while the eavesdropper obtains the entire secret key. We propose a new theoretical approach called quantum flows to be able to detect the eavesdropping activity in the channel without requiring additional optical components different from the BB84 protocol because the system can be implemented as a high software module. In this approach, the transmitter interleaves pairs of quantum states, referred to here as parallel and orthogonal (non-orthogonal) states, while the receiver uses active basis selection.

Keywords: quantum key distribution, photon number splitting attack, intercept resend faked states attack

1. Introduction

Quantum key distribution (QKD) is a technique to distribute securely a cryptographic key between two remote users, usually called Alice and Bob. The first *QKD* method was conceived by Charles Bennett and Gilles Brassard in 1984, usually referred to in literature as *BB84* [1]. **Figure 1** shows a simplified representation of the two-dimensional Bloch sphere, the quantum states, and the measurement bases of *BB84*.

QKD systems are designed to serve the purpose of generating secret bits, usable to encrypt plain-text messages based on a simple $X - Or$ logical function between the message and a secret key. The use of this system provides the availability to detect any eavesdropper, commonly called Eve, trying to intercept the quantum channel to get the key. In this case, the

IntechOpen

© 2018 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

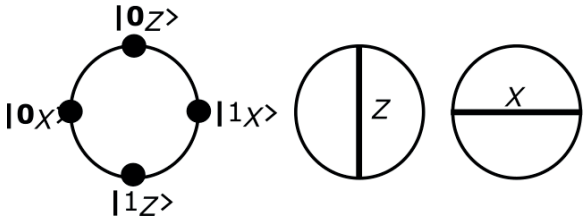

Figure 1. The *BB84* qubits are the *non-orthogonal* states: the measurement bases, Z and X, are shown as vertical and horizontal lines, correspondingly. When basis X (Z) is used by Bob, to measure Alice's state $|i_X\rangle$ ($|i_Z\rangle$), the result gotten by Bob is bit i ($i = 0, 1$); otherwise, if basis X (Z) is applied to measure $|i_Z\rangle$ ($|i_X\rangle$) the probability to get i reduces to $\frac{1}{2}$. So, if Bob measures the $|0_X\rangle$ state with Z basis, he has the same probability to obtain $|0_Z\rangle$ or $|1_Z\rangle$.

whole process will be discarded before a key can be established [2]. On the other hand, if no eavesdropping activity is detected, the quantum measurements are used to derive the secret key. When the transmission is finished, Alice and Bob compare a fraction of the exchanged key in order to detect any transmission errors caused by eavesdropping. Experimentally, *QKD* systems have been proved using dedicated optical fibers, across free space, weak laser pulses or single photons, entangled photon pairs, or continuous variables [3].

We propose a new approach for *QKD* protocols called quantum flows where the transmitter interleaves pairs of quantum states, referred to here as *parallel* and *orthogonal* (*non-orthogonal*) states, while the receiver applies active basis selection to perform state measurement. In a study by Lizama et al. [4], a brand new *QKD* protocol, called *ack-state* and referred to also as *ack-QKD*, is introduced. This protocol uses weak coherent states and active basis measurement and has the capability to detect photon number splitting *(PNS)* eavesdropping activity, and its strengths against the *PNS* attack are discussed by Lizama-Pérez et al. [5]. The *ack-state* protocol was extended by Lizama-Pérez et al. [6] to the dual protocol known as *nack state* protocol in order to have an analysis of its security when facing an intercept and resend with faked states *(IRFS)* attack.

One of the main advantages of these protocols is that they protect against the *PNS* and the *IRFS* attacks without requiring any changes in the hardware; only software changes are required.

2. Quantum hacking in *QKD* systems

In ideal conditions, QKD protocols' security is based on the attributes of quantum mechanics, as it makes eavesdropping activities detectable in the middle of the quantum channel [1, 7]. But the technological implementation brings serious concerns as most of the *QKD* systems have vulnerabilities to quantum hacking due to loopholes in the optical detection system [8–18]. Given this condition, it is necessary to develop new *QKD* protocols that are able to resist different attacks due to such vulnerabilities as the photon number splitting (*PNS*) and the intercept and resend with faked states (*IRFS*) attacks [19, 20].

A variety of attacks have been conceived of as exploiting the security of *BB84*-based systems, either theoretically or technologically. The photon number splitting (*PNS*) attack belongs to the first category. In the second class, commonly referred to as quantum hacking, the intercept resend with faked states (*IRFS*) attack can be included, which exploits loopholes in the avalanche photo diodes (*APD*s) of the electronic detection system. We will briefly describe each of them.

1. In the *PNS* attack the eavesdropper blocks the 1-photon states but she stores the multi-photon states allowing at least one photon to reach Bob's detection system. Ideally, in the *BB84* protocol [1], the quantum states sent by Alice to Bob contain single photons. Nevertheless, perfect single photon sources are not technologically available nowadays [21], so, to get the implementation of *QKD*, laser pulses attenuated to very low levels have been used. Such laser pulses contain very short numbers of photons, in average typically around 0.2 photons per pulse in a Poissonian distribution; that means that most pulses contain no photons, a few pulses contain just one photon, and a really short amount of pulse contains two or more photons. If a pulse contains more than one photon, Eve can get from it the extra photons and transmit a single photon to Bob. Eve can store the photons she obtained from the multi-photonic pulses and wait until Bob reveals the measurement basis he has applied. Then Eve can measure the photons she stored by using the same measurement basis as Bob did. In this way she obtains information about the key without being noticed by Alice and Bob. This is called the photon number splitting (*PNS*) attack, and some related references with security proofs of the *PNS* attack can be found in [1, 7, 22–24].

   To overcome the PNS attack a few protocols have been developed: Decoy QKD [18], SARG04 [25], the differential phase shift (DPSK) [26], and coherent one way (COW) [27]. One of the most promissory alternatives is the decoy QKD. In this protocol Alice prepares a set of quantum states in addition to the typical states of the BB84 protocol. These extra states are called decoy states. Decoy states are used only with the purpose to detect the eavesdropping activity, rather than establishing the key. In order to produce the decoy states, Alice randomly uses different mean photon numbers on the photonic source. For example, she could send the first pulse with a mean photonic pulse of $\mu = 0.1$, the second pulse with $\mu = 0.4$, the third pulse with $\mu = 0.05$, and so on. To each mean photon number a different probability of producing more than one photon in the correlated pulse corresponds. The difference between the standards BB84 states and the decoy states is the mean photon numbers. Given this, Eve is not able to distinguish a decoy state from a quantum key related state and the only information she gets is the number of photons in a pulse. Thus, decoy states can be introduced to secure the BB84 protocol from PNS attacks, allowing at the same time high key rates. In both, BB84 and decoy QKD protocols, a single photonic gain in the quantum channel is established. Lamentably, Eve can set successful attacks to the decoy QKD if it is able to set the QBER to zero by adjusting the gain of the quantum channel.

2. Intercept Resend (*IR*) attack: In this attack, Eve measures each photon pulse sent by Alice and replaces it with a different pulse prepared in the quantum state that she has

previously measured. In 50% of the measurements, Eve successfully chooses the correct measurement basis, while Bob chooses the same basis as her half of the time. Given that, she generates a quantum bit error rate (*QBER*) of $50\% \times 50\% = 25\%$ (see **Figure 2** and a study by Bennett et al. [7]).

3. Intercept resend with faked states (*IRFS*) attack.

In the intercept resend with faked states (IRFS) attack, the eavesdropper does not want to reconstruct the original states. Instead, it produces pulses of light controlled by her that are detectable by Bob as she stays unnoticed in the quantum channel. Due to imperfections in their optical system, Alice and Bob assume that the quantum states they are detecting are the original ones while they are actually detecting light pulses generated by the eavesdropper. Those light pulses are known as faked states [10]. There are several weaknesses in Bob's detector than can be exploited to perform this attack such as time shift [11–13] or quantum blinding [10–12]. When using quantum blinding (quantum blinding attack), the QKD system is controlled by an eavesdropper who uses bright photon pulses during the linear mode operation of the APDs. Using this attack, Eve can eavesdrop on the full secret key but it will not increase the QBER of the protocol. To do this, Eve sends bright pulses to Bob and those are detected by the APD. It will then operate like a classical photo diode instead of operating in Geiger mode and allowing Eve to obtain the key [14, 15].

Resulting from this, as shown in **Figure 3a**, when Bob selects the same measurement basis Eve has chosen, a detection event occurs in the corresponding APD detector. On the other hand, if Bob measures using the opposite basis, as in **Figure 3b**, the two detectors get a part of the optical power and no event is detected. In this way, the eavesdropper blinds Bob's APD detectors and makes them work as classical photo diodes. In the final stage of the protocol, Eve uses the announcements made by Bob on the public channel to execute the classical post-processing, getting the same secret bit as Alice and Bob.

A watchdog detector that can detect bright faked states can be used as a very simple countermeasure and it can be applied in the electronic detection system [16]. In the University of Singapore an intercept resend attack with faked states and quantum blinding over a commercial QKD system was for the first time implemented [15].

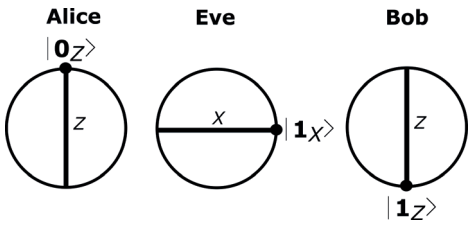

Figure 2. An intercept resend (*IR*) attack toward the *BB84* protocol causes a quantum bit error rate (*QBER*) of 25% that can be detected. The figure shows Alice sending a $|0_Z\rangle$ state to Bob. In the middle of the quantum channel is Eve applying an *X* basis measurement and she gets $|1_X\rangle$. Consequently, she makes a copy of that state and sends it to Bob who gets $|1_Z\rangle$ as he used the *Z* basis measurement. The process introduces an error in the secret bit given that Alice expects Bob to get $|0_Z\rangle$.

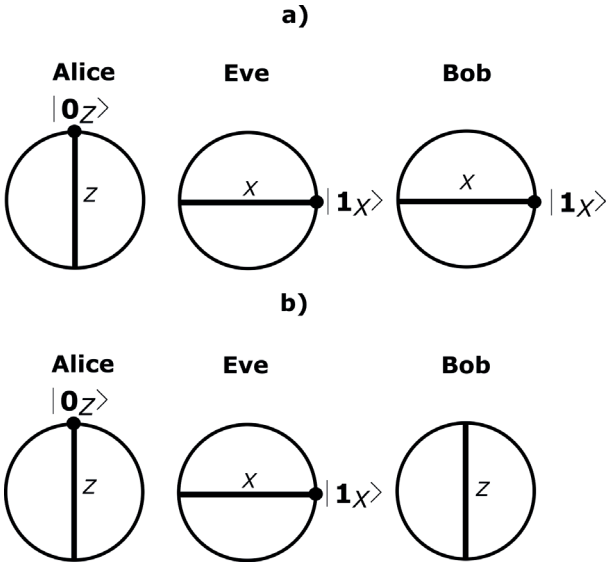

Figure 3. In the intercept resend with faked states (*IRFS*) and quantum blinding attack, Eve and Bob use the same optical receiver unit so that she can detect Alice's states in a random basis. Then, Eve prepares the quantum states but sends them to Bob as bright light pulses instead of quantum pulses. (a) Bob and Eve are using the same basis; (b) the basis Bob is using is the opposite to ve.

It is important to note that the *IRFS* attack works dangerously well on widely used QKD protocols, namely *SARG04*, *BB84*, coherent one way (*COW*), differential phase shift (*DPSK*), Ekert [12], and the *decoy state* method, as described by Wiechers et al. [16] and Sun et al. [28]. The attack shows an extra 3 dB loss due to the basis of mismatch between Eve and Bob. In the practice, Eve compensates it easily as she can use better detector efficiencies and surpass the loss in the channel. Demonstrations of blinding attacks on detectors have been implemented in two commercially available *QKD* systems [14]. Reports show that Eve obtains the entire secret key for the time she remains unnoticed by the legitimate parties [15]. We should finally remark that due to control detector attacks with active basis selection, the gain from Eve to Bob is reduced by a half compared to the gain from Alice to Bob.

i. *For Bob's basis choice matching Eve's, the detector clicks deterministically and.*

ii. *For Bob's basis choice not matching Eve's, the faked state is not detected.*

3. The *ack-state* protocol

Consider a *BB84*-based protocol encoding a classical bit that uses one of the four *non-orthogonal* quantum states $|+_X\rangle, |-_X\rangle, |+_Z\rangle$, and $|-_Z\rangle$ (see **Figure 1**). When using the *SARG04* protocol [25], Alice produces one of the four *BB84* quantum states she will send to Bob, it means, she produces a state associated with two conjugate basis (X and Z). Classical bits on *SARG04*

protocol are encoded as follows: 0 is coded with$|+_Z\rangle$ and $|-_Z\rangle$ and 1 is coded with $|+_X\rangle$ and $|-_X\rangle$ (see **Figure 4**) where black dots in the bidimensional Bloch sphere represent the qubits (the *non-orthogonal* states are right angled and the *orthogonal* states are represented as diametrically opposed and the *parallel* states have the same position in the sphere). The basis measurement X and Z appear as horizontal and vertical lines, respectively. In contraposition, the *BB84* protocol encodes the bit 0 as $|+_Z\rangle$ and $|-_X\rangle$ and the bit 1 with $|-_Z\rangle$ and $|+_X\rangle$.

In the sifting phase of the *SARG04* protocol, the basis used by Alice is not revealed as this would reveal the bit. As a substitute, she declares to which sifting set the state belongs in accordance with the following four sifting sets: $S_{(+,+)} = \{|+_X\rangle, |+_Z\rangle\}$, $S_{(+,-)} = \{|+_X\rangle, |-_Z\rangle\}$, $S_{(-,+)} = \{|-_X\rangle, |+_Z\rangle\}$, and $S_{(-,-)} = \{|-_X\rangle, |-_Z\rangle\}$. For instance, consider that Alice sends $|+_X\rangle$ and she announces the set $S_{(+,+)}$. Bob makes his measurements on the X basis and he gets the

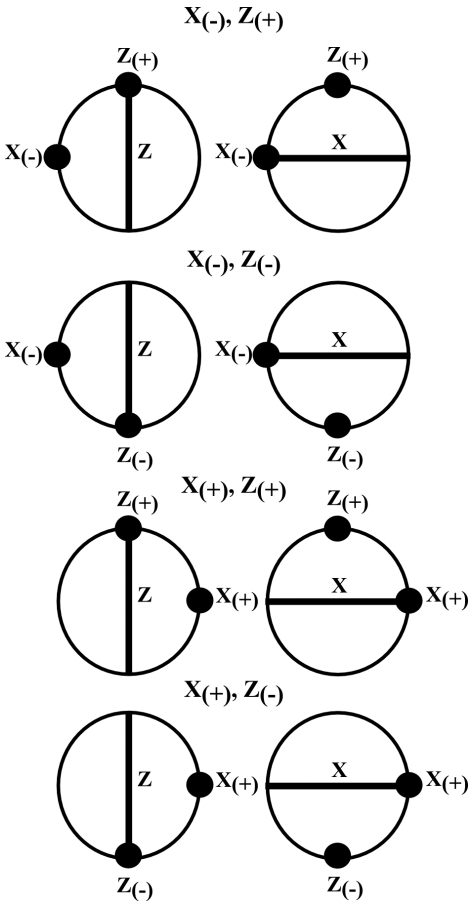

Figure 4. The *non-orthogonal* states used in the *SARG04* protocol encodes the bit 0 with the states $|+_Z\rangle$ and $|-_Z\rangle$ and the bit 1 is encoded with $|+_X\rangle$ and $|-_X\rangle$.

result $|+_X\rangle$; and as this result can be obtained for both states in the set $S_{(+,+)}$; he needs to dispose of the bit 1 from $|+_X\rangle$. In case Bob measures using the Z basis measurement and obtains $|+_Z\rangle$, once more, he is not able to distinguish the state sent by Alice. In the opposite way, if he measures in the Z basis and gets $|-_Z\rangle$, he is sure Alice sent $|+_X\rangle$ and adds a 0 to his key. On her side, Eve needs to perform a measurement using the conjugate basis X and Z to obtain the same secret bit as Bob, demanding multi-photonic pulses with at least three photons.

Similar to the *BB84*, in the *ack-state* protocol, Alice encodes a classical bit as: 0 is encoded with $|+_Z\rangle$ and $|-_X\rangle$ and 1 is encoded with $|-_Z\rangle$ and $|+_X\rangle$. And also, in the same manner as the *SARG04* protocol, the *ack-state* uses the four sets of *non-orthogonal* states $S_{(+,+)} = \{|+_X\rangle, |+_Z\rangle\}$, $S_{(+,-)} = \{|+_X\rangle, |-_Z\rangle\}$, $S_{(-,+)} = \{|-_X\rangle, |+_Z\rangle\}$, and $S_{(-,-)} = \{|-_X\rangle, |-_Z\rangle\}$. But in the *ack-state* protocol the set Alice used, $S_{(+,+)}$, $S_{(+,-)}$, $S_{(-,+)}$ or $S_{(-,-)}$, is never revealed. As an illustration, suppose Alice chooses the set $S_{(+,+)} = \{|+_X\rangle, |+_Z\rangle\}$ rather than transmitting one of the two states, say $|+_X\rangle$, and publishing the sifting instance, $S_{(+,+)}$, she transmits the two states $|+_X\rangle$ and $|+_Z\rangle$. At that point, Bob measures the states using the same basis, X or Z, one by one, as the two states reach successively. If Bob measures with the X basis, he surely will obtain $|+_X\rangle$ (after he measures the first state) but he can obtain $|+_X\rangle$ or $|-_X\rangle$ on the second measurement, with a probability of 0.5 for each event. If Bob obtains $\{|+_X\rangle, |-_X\rangle\}$ after the second measurement, the result is unclear to him and he has to discard it. On the other hand, if he gets $\{|+_X\rangle, |+_X\rangle\}$ the result is unambiguous and he should add a bit 1 to his key. With the purpose of allowing Alice to recover the same bit, Bob makes the announcement of the basis measurement X and the matching condition in accordance with the following criterion: $(2M)$ if the two detection events make clicks on the same detector; it includes the cases $\{|+_X\rangle, |+_X\rangle\}$, $\{|-_X\rangle, |-_X\rangle\}$, $\{|+_Z\rangle, |+_Z\rangle\}$, $\{|-_Z\rangle, |-_Z\rangle\}$ and $(2nM)$ if the detection event makes clicks on the opposite detectors, for example, $\{|+_X\rangle, |-_X\rangle\}$, $\{|-_X\rangle, |+_X\rangle\}$, $\{|+_Z\rangle, |-_Z\rangle\}$, $\{|-_Z\rangle, |+_Z\rangle\}$. Alice obtains the secret bit given that the $\{|+_X\rangle, |+_Z\rangle\}$ states she sent, the X basis, and the $(2M)$ measurement result permit her to conclude that Bob definitely got $\{+_X, +_X\}$ (consider the cases depicted in **Table 1**).

Contrarily, in the case Bob measured the two states $|+_X\rangle$ and $|+_Z\rangle$ with the Z basis, he would acquire one of the two possible results: $(2M) = \{|+_Z\rangle, |+_Z\rangle\}$ or $(2nM) = \{|-_Z\rangle, |+_Z\rangle\}$. In the first case, he publishes the Z basis and the $(2M)$ result; then Alice and Bob add a 0 to the key. In the second case, Bob makes the announcement of the Z basis and the $(2nM)$ result but in this case, they discard the result. When using the *ack-state* protocol the $(2M)$ results can be used to

Alice sends	**Bob obtains a $(2M)$**	**Secret bit**
$\{|+_X\rangle, |+_Z\rangle\}$	$\{|+_X\rangle, |+_X\rangle\}$	1
$\{|+_X\rangle, |-_Z\rangle\}$	$\{|+_X\rangle, |+_X\rangle\}$	1
$\{|-_X\rangle, |+_Z\rangle\}$	$\{|-_X\rangle, |-_X\rangle\}$	0
$\{|-_X\rangle, |-_Z\rangle\}$	$\{|-_X\rangle, |-_X\rangle\}$	0

Table 1. Using the X basis, Bob measures the two states sent by Alice and he obtains a $(2M)$ result.

distill secret bits but $(2nM)$ is unclear causing those measurement outcomes to be useless and so they have to be discarded.

The *ack-state* protocol was introduced in [4]. In such a reference, the *non-orthogonal* states are called *protocol* states while *parallel* states are named *decoy* states. The *ack-state* protocol encodes one classical bit using two quantum states. Such encoding is done by means of *non-orthogonal* or *parallel* states. In quantum physics, if $X = \{|0_X\rangle, |1_X\rangle\}$ and $Z = \{|0_Z\rangle, |1_Z\rangle\}$ are orthonormal bases, then the magnitude of each basis vector is the unity and any vector in such a space can be written as a linear combination of such basis. For instance, $|0_X\rangle$ can be rewritten as $\frac{1}{\sqrt{2}}|0_Z\rangle + \frac{1}{\sqrt{2}}|1_Z\rangle$. Two qubits $|0_X\rangle$ and $|0_Z\rangle$ are *non-orthogonal* if the inner product between them is different from zero, symbolically $0_X|0_Z \neq 0$. In consequence, $0_X|0_Z = \frac{1}{\sqrt{2}}(1) + \frac{1}{\sqrt{2}}(0)$ and $0_X|0_Z = \frac{1}{\sqrt{2}}$. The inner product of *orthogonal* qubits is zero, for example, $0_X|1_X = 0$ and identical (or *parallel*) qubits produce the unity under the inner product; thus, $0_X|0_X = 1$.

Using this protocol, Alice chooses at random between sending a pair of *parallel* or *non-orthogonal* states. At the opposite side, Bob makes the measurement of the two successive pulses he receives with the same basis measurement, X or Z (see **Figure 5**). In this context, the pair of quantum states sent by Alice is called biqubit. *Parallel* biqubits define the *parallel* quantum flow and *non-orthogonal* biqubits define the *non-orthogonal* quantum flow. Summarizing the *ack-state* protocol with *non-orthogonal* and *parallel* states, we have the following:

1. Alice randomly selects between a *non-orthogonal* biqubit and a *parallel* bi-qubit. In case she selects a *non-orthogonal* biqubit, she has to select at random one of the following states: $\{(|0_X\rangle, |0_Z\rangle), (|0_X\rangle, |1_Z\rangle), (|1_X\rangle, |0_Z\rangle), (|1_X\rangle, |1_Z\rangle)\}$, where the order between states X or Z is as well picked at random. In case she selects a *parallel* biqubit, she should randomly choose a biqubit from the set: $\{(|0_X\rangle, |0_X\rangle), (|1_X\rangle, |1_X\rangle), (|0_Z\rangle, |0_Z\rangle), (|1_Z\rangle, |1_Z\rangle)\}$. and then she gets it ready and transmits it to Bob.

2. At random, Bob chooses the basis X or Z to measure the received biqubit.

3. Bob's basis of measurement is announced by him over the public channel and he also declares if the result obtained is either a double-detected event ($2M$ or $2nM$), a single-detected event (S-1 or S-2), or a lost biqubit $(2L)$ (see the discussion below).

4. After analyzing those results, Alice tells Bob which cases to discard.

Table 2 shows the results after Bob measures two consecutive states. Thus, one of the following detection events can be obtained:

i. *The states generate a double-detection event:* The symbol $(+,+)$ is used to designate the photonic gain in a double-detection event. When both events are registered in a same detector, we call it a double-matching $(2M)$ detection event. If the results of the measurements of the states are opposite, then we face a double non-matching $(2M)$ detection event. Whereas $(2M)$ *non-orthogonal* outcomes are useful to distill secret bits, the $(2M)$ results cannot be used and are disposed. When we have a $(2M)$ detection event, we may say that the second measurement is the acknowledgment (the *ack*) of the first measurement. In **Figure 5** (top-right) the qubit $|0_X\rangle$ is the first one sent by Alice and then she sends

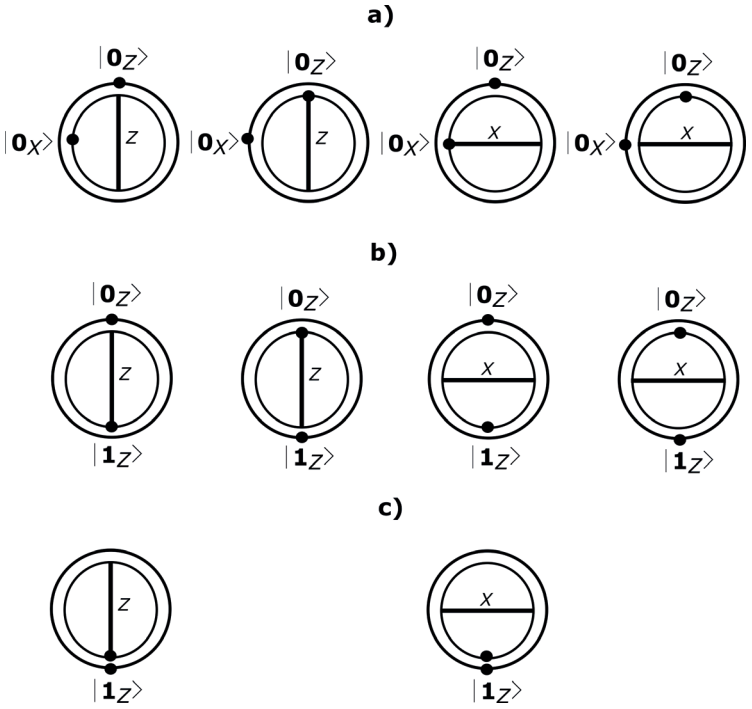

Figure 5. In this representation, two concentric circles define the order in which the states are prepared and sent. Therefore, the state that is first sent is contained in the inner circle state, and the outer circle state is prepared and transmitted. Alice at random interleaves *orthogonal* (*non-orthogonal*) and *parallel* states, given that she can verify the matching cases after Bob measurements. In the *ack-state* protocol, Bob uses the basis $X(Z)$ to measure the two Alice's *non-orthogonal* states $\{|i_X\rangle, |j_Z\rangle\}$. He effectively gets the bit $i(j)$ provided he measures $\{|i_X\rangle, |i_X\rangle\}$ or $\{|j_Z\rangle, |j_Z\rangle\}$ which occurs with $\frac{1}{2}$ probability. For instance, if Bob uses the Z basis to measure the incoming states $\{|0_X\rangle, |1_Z\rangle\}$ he can obtain $\{|0_Z\rangle, |1_Z\rangle\}$ or $\{|1_Z\rangle, |1_Z\rangle\}$ with the same probability. Alice decides to send at random two consecutive *non-orthogonal* states from the set: $\{(|0_X\rangle, |0_Z\rangle), (|0_X\rangle, |1_Z\rangle), (|0_Z\rangle, |1_X\rangle), (|1_Z\rangle, |1_X\rangle)\}$. Bob will measure those states using the same measurement basis (X or Z). The *parallel* biqubits involve the following states: $\{(|0_X\rangle, |0_X\rangle), (|1_X\rangle, |1_X\rangle), (|0_Z\rangle, |0_Z\rangle), (|1_Z\rangle, |1_Z\rangle)\}$. In the *nack-state* protocol Alice chooses randomly two consecutive *parallel* states as the case depicted in (c) $(|1_Z\rangle, |1_Z\rangle)$. They produce a compatible measurement if Bob chooses, X for $|i_X\rangle$ or Z for $|i_Z\rangle$ where $i = 0, 1$. We represent in (b) the case of quantum *orthogonal* states. Two cases are possible here: $\{(|0_X\rangle, |1_X\rangle), (|0_Z\rangle, |1_Z\rangle)\}$.

the qubit $|0_Z\rangle$. As the X basis is used by Bob to measure both qubits, the qubit $|0_X\rangle$ is measured as $|0_X\rangle$ but the qubit $|0_Z\rangle$ is measured as $|0_X\rangle$ or $|1_X\rangle$ with an equal probability of 50%. When Bob's measurement generates $|0_X\rangle$, we say that this measurement is the *ack* of the first $|0_X\rangle$ state. Vice versa, if Bob gets $|1_X\rangle$, we say that $|1_X\rangle$ is the negative acknowledgment (the *nack*) of $|0_X\rangle$.

In a *channel* with losses, we have two more possible results.

ii. *The single-detection event* occurs when one state is lost and Bob obtains only one detection event. The symbol $(\pm, \mp)$ is used to designate the single-detection event. More specifically, Bob uses the symbol $(S\text{-}i)$ to represent the single-detection event, where i can be 1 or

Alice's bi-qubit	Bob's side			
	basis used	Detection event	Public disclosure	Result
$\|0_X\rangle, \|0_Z\rangle$	X	$\|0_X\rangle, \|0_X\rangle$	$X, (2M)$	Useful
	X	$\|0_X\rangle, \|1_X\rangle$	$X, (2nM)$	Discard
	X	$\|0_X\rangle, -$	$X, (S\text{-}1)$	Useful
	X	$-, \|0_X\rangle$	$X, (S\text{-}2)$	Discard
	X	$-, \|1_X\rangle$	$X, (S\text{-}2)$	Discard
	X	$-, -$	$X, (2L)$	Discard
	Z	$\|0_Z\rangle, \|0_Z\rangle$	$X, (2M)$	Useful
	Z	$\|1_Z\rangle, \|0_Z\rangle$	$X, (2nM)$	Discard
	Z	$-, \|0_Z\rangle$	$Z, (S\text{-}2)$	Useful
	Z	$\|0_Z\rangle, -$	$Z, (S\text{-}1)$	Discard
	Z	$\|1_Z\rangle, -$	$Z, (S\text{-}1)$	Discard
	Z	$-, -$	$Z, (2L)$	Discard

Table 2. Alice sends to Bob the *non-orthogonal* states $(|0_X\rangle, |0_Z\rangle)$ and it shows all the possible measurement results at Bob's side.

2, depending on the state number that makes clicks after the basis measurement X or Z is applied to the two consecutive incoming states. This way, the number i will be published by Bob.

iii. *The two pulses are lost.* This case is denoted as $(-, -)$ or alternatively as $2L$.

When applying the *ack-state* protocol, two consecutive *non-orthogonal* states are used by Alice and Bob to distill one secret bit. The basis measurement X or Z is declared publicly by Bob along with the sifting instances; he obtained $(2M)$, $(2M)$, $(S\text{-}1)$, $(S\text{-}2)$, and $(2L)$. Furthermore, the bits acquired from the single-detection events $(S\text{-}1)$ and $(S\text{-}2)$ are used by Alice to confirm the single photonic gain of the quantum channel.

4. The *nack-state* protocol

The *nack-state* protocol is the dual version of the *ack state* protocol discussed in [5]. Both protocols constitute a generalization of the well-known *BB84*. The *nack state* protocol uses couples of *parallel* and *orthogonal* states rather than just single *non-orthogonal* states utilized as a part of *BB84*. This straightforward distinction makes the *nack state* strong when facing the *IRFS* attack, as we will demonstrate later on. We selected the *nack* prefix to indicate that, provided Alice transmits two quantum states to Bob, the second measurement behaves as the negative acknowledgment (*nack*) of the one before, since it yields the opposite bit result.

The pair of quantum states is denoted as a biqubit. More specifically, the following biqubits are defined in the *nack state* protocol: four *parallel* biqubits $(|0_X\rangle, |0_X\rangle), (|0_Z\rangle, |0_Z\rangle), (|1_X\rangle, |1_X\rangle),$

$(|1_Z\rangle, |1_Z\rangle)$ and two *orthogonal* biqubits $(|0_X\rangle, |1_X\rangle), (|0_Z\rangle, |1_Z\rangle)$. The *parallel* and *orthogonal* biqubits are interleaved at random by Alice. The performance of the protocol is not altered by order of the quantum states within the biqubit (see **Figure 5**). On the opposite side of the

Alice's	Bob's	Detection	Public	Description
Biqubit	Basis	Event	Disclosure	
	X	$\|0_X\rangle, \|1_X\rangle$	$X, 2nM$	Compatible double non-matching, useful
				As two compatible single-detection events
	X	$\|0_X\rangle, -$	X, S_1	Compatible single matching, useful
	X	$-, \|1_X\rangle$	X, S_2	Compatible single matching, useful
	X	$-, -$	X, Lost	Biqubit lost
	Z	$\|0_Z\rangle, \|0_Z\rangle$	$Z, 2M$	Non-compatible double matching, useless
	Z	$\|1_Z\rangle, \|1_Z\rangle$	$Z, 2M$	Non-compatible double matching, useless
$\|0_X\rangle, \|1_X\rangle$	Z	$\|0_Z\rangle, \|1_Z\rangle$	$Z, 2M$	Non-compatible double non-matching, useless
	Z	$\|1_Z\rangle, \|0_Z\rangle$	$Z, 2M$	Non-compatible double non-matching, useless
	Z	$\|0_Z\rangle, -$	Z, S_1	Non-compatible single matching, useless
	Z	$\|1_Z\rangle, -$	Z, S_1	Non-compatible single matching, useless
	Z	$-, \|0_Z\rangle$	Z, S_2	Non-compatible single matching, useless
	Z	$-, \|1_Z\rangle$	Z, S_2	Non-compatible single matching, useless
	Z	$-, -$	Z, Lost	Biqubit lost
	Z	$\|1_Z\rangle, \|1_Z\rangle$	$Z, 2M$	Compatible double matching, useful
	Z	$\|1_Z\rangle, -$	Z, S_1	Compatible single matching, useful
	Z	$-, \|1_Z\rangle$	Z, S_2	Compatible single matching, useful
	Z	$-, -$	Z, Lost	Biqubit lost
	X	$\|0_X\rangle, \|0_X\rangle$	$Z, 2M$	Non-compatible double matching, useless
	X	$\|1_X\rangle, \|1_X\rangle$	$Z, 2M$	Non-compatible double matching, useless
$\|1_Z\rangle, \|1_Z\rangle$	X	$\|0_X\rangle, \|1_X\rangle$	$Z, 2nM$	Non-compatible double non-matching, useless
	X	$\|1_X\rangle, \|0_X\rangle$	$Z, 2nM$	Non-compatible double non-matching, useless
	X	$\|0_X\rangle, -$	X, S_1	Non-compatible single matching, useless
	X	$\|1_X\rangle, -$	X, S_1	Non-compatible single matching, useless
	X	$-, \|0_X\rangle$	X, S_2	Non-compatible single matching, useless
	X	$-, \|1_X\rangle$	X, S_2	Non-compatible single matching, useless
	X	$-, -$	X, Lost	Biqubit lost

We expect Alice to send the biqubits $|0_X\rangle, |1_X\rangle$ and $|1_Z\rangle, |1_Z\rangle$; at that point, every conceivable measurement result at Bob's detector is written. We exhibit the detection event and Bob's corresponding advertisement over the public channel according to Bob's basis selection. Notice that the number of the single detections inside the biqubit, first or second, is openly declared by Bob.

Table 3. The *nack-state* protocol running without blunders in the quantum channel is shown with each of the possible measurement results at Bob's detectors.

quantum channel, Bob measures two incoming states of a biqubit utilizing the same measurement basis (X or Z). The following steps depict the *nack state* protocol:

1. Alice is equipped with a photon source with an expected photon number μ showing Poisson distribution. A *parallel* or an *orthogonal* biqubit is selected at random by Alice, and she arranges the biqubit to be sent to Bob through the quantum channel.
2. The biqubit (two incoming pulses) is measured by Bob using the same measurement basis X (or Z) that he selects haphazardly (in a further section, we discuss the convenience of avoiding consecutiveness of states and how it can be prevented if Alice forwards a burst of the first states of each pair, followed by a burst of the second states of each pair).
3. Bob declares publicly his measurement basis decisions.
4. Alice and Bob perform sifting utilizing single compatible events and double compatible matching detection events (from *parallel* states) in order to share secret bits. Likewise, sifting is applied to the double-detection events that contain a single compatible detection event. With this aim, Bob indicates if the single detection is the first or the second inside the biqubit.

Table 3 exhibits a case of the *nack state* protocol. Here, two biqubits are transmitted to Bob from Alice. The first biqubit is the *orthogonal* pair $(|0_X\rangle, |1_X\rangle)$, and the second biqubit is the *parallel* pair $(|1_Z\rangle, |1_Z\rangle)$. In case the two states sent by Alice reach Bob's detection system with no failure, a double-detection event is generated. In the situation that just one of the two states of the biqubit reaches Bob's station, he gets a single-detection event.

The *nack-state* protocol has been conceived of to use the same optical hardware of the *BB84* protocol; thus, it can be configured in most *QKD* systems as a software module application. However, two additional tasks must be implemented: the random computation of biqubits before preparing and sending the quantum states and the sifting stage of the protocol, which must include (1) sifting of single matching (compatible or non-compatible), where Bob announces the number of the single-detections inside the biqubit and (2) sifting of double detection, matching or non-matching, from *parallel* or *orthogonal* states. The error correction and privacy amplification stages of the *QKD* protocol do not require changes.

5. The photon number splitting attack

In the *PNS* attack, the eavesdropper captures no less than one photon from each of the multi-photon states with the purpose of storing them in quantum memory, at the same time that she hinders the single photon states in the quantum channel. When Bob has uncovered over public channels the measurement basis he has used, the eavesdropper executes the same measurements on the quantum states she has stored [25].

When the *PNS* attack is applied to the *ack-state* protocol, the eavesdropper captures no less than one photon of the multi-photon states (*parallel* and *non-orthogonal*), and she stands by Bob's declarations about the measurement bases he has utilized with the aim of applying the

same measurements on her stored states. In Bob's side, a distribution over the following sifting events is achieved $(2M)$, $(2nM)$, $(S\text{-}1)$, $(S\text{-}2)$ and $(2L)$, where every one may originate in *parallel* or *non-orthogonal* states; however, just Alice knows those outcomes.

After Bob declares both the measurement bases (X or Z) and the sifting occurrences, Eve executes the measurements utilizing the same measurement bases and she gets the same bits from the multi-photonic single sifting instances: $(S\text{-}1)$ and $(S\text{-}2)$, *parallel* and *non-orthogonal*. Moreover, the same outcomes from the $(2M)$ measurements of the *parallel* and (a half of the) *non-orthogonal* multi-photonic states are acquired by the eavesdropper. However, she cannot acquire the secret bits from the 1-state $(S\text{-}i)$ and $(2M)$ sifting occurrences, given that the eavesdropped cannot discriminate *parallel* and *non-orthogonal* states.

In order to get the secret bits, Eve obstructs the 1-photon states which incorporate single and double-detection events from *parallel* and *non-orthogonal* states. In doing that, an error gain in the photonic gain of the single and double-detection events is introduced by Eve. At that point, Eve executes a channel substitution expanding the transmittance of the channel. The fiber channel transmittance among Alice and Bob is written as $T_{AB} = 10^{-\frac{\alpha l}{10}}$ where α is the loss coefficient measured in dB/km and the length l is measured in km. Moreover, the local transmittance at Bob's side, η_B, is defined as $t_B\eta_D$ where t_B is the internal transmittance of optical components and η_D is the quantum efficiency of Bob's detectors. Then, the general transmission and detection efficiency at Bob's side η_{BT} is computed as $\eta_{BT} = t_B\eta_D T_{AB}$ [18]. A mathematical description of the gain of detection events will be presented in the following section.

5.1. The gain of detection events

In **Table 4** (upper part), the gain of the single-detection events is depicted with the $Q_{(+)}$ symbol. According to Ma et al. [18], the gain of detection events is acquired from two origins: the photon source and the quantum channel. The photon source presents an expected photon number μ, and it adopts Poisson distribution. Contrastively, the quantum channel exhibits a distribution that is computed for every i photons' state (where i is the quantity of photons in each pulse) that is named yield. The gain Q_i of i photons' state is the product of the probability of Alice sending an i photons' state (that adopts Poisson distribution) and the yield of i photons' state (and background states). It will generate a gain at Bob's side provoked by the detection of events corresponding to the relation $Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}$ where Y_i is the yield of i photons' state.

The yield Y_i is computed across the following steps:

1. The fiber channel transmittance among Alice and Bob is denoted as $T_{AB} = 10^{-\frac{\alpha l}{10}}$ where α is the loss coefficient measured in dB/km, and the length l is measured in km. Moreover, the local transmittance at Bob's side, η_B, is written as $t_B \cdot \eta_D$ where t_B is the internal transmittance of optical components and η_D is the quantum efficiency of Bob's detectors. Then, the overall transmission and detection efficiency at Bob's side, η_{BT}, is computed as $\eta_{BT} = t_B \cdot \eta_D \cdot T_{AB}$ and typically η_{BT} ranges to 10^{-3} [18];

Photonic-Gain	Alice	Alice − Bob	Eve − Bob
$Q_{(-)}$	$e^{-\mu}$	$e^{-\mu\eta_{BT}} - Y_0$	—
$Q_{(+)}$	$1 - e^{-\mu}$	$Y_0 + 1 - e^{-\mu\eta_{BT}}$	$\frac{1}{2}(Y_0 + 1 - e^{-\mu\eta_{ET}})$
$Q_{(-,-)}$	$e^{-2\mu}$	$(e^{-\mu\eta_{BT}} - Y_0)^2$	—
$Q_{(\pm,\mp)}$	$2e^{-\mu}\cdot$	$2(e^{-\mu\eta_{BT}} - Y_0)\cdot$	$(e^{-\mu\eta_{ET}} - Y_0)\cdot$
	$(1 - e^{-\mu})$	$(Y_0 + 1 - e^{-\mu\eta_{BT}})$	$(Y_0 + 1 - e^{-\mu\eta_{ET}})$
$Q_{(+,+)}$	$(1 - e^{-\mu})^2$	$(Y_0 + 1 - e^{-\mu\eta_{BT}})^2$	$\frac{1}{2}(Y_0 + 1 - e^{-\mu\eta_{ET}})^2$

Here, η_{BT} and η_{ET} are the overall efficiency of Bob and Eve, respectively. In the *IRFS* attack, Eve remains undetected given that she meets the condition $\eta_{ET} \geq \frac{\ln(2e^{-\mu\eta_{BT}} - Y_0 - 1)}{-\mu}$. At the lower part of the table, the gain of the double $(+,+)$-detection events is shown, which is denoted as $Q_{(+,+)}$, and the gain of single $(\pm, \mp)$ detection events is represented as $Q_{(\pm,\mp)}$. In the *IRFS* attack, Eve can effectively forward half of her biqubits to Bob's detectors. The "$\cdot$" symbol denotes multiplication inside the $Q_{(\pm,\mp)}$ relation. The factor of 1/2 is a result of Bob using an active basis choice, compelling Eve to blind his detector when his basis differs from her own (half the time), and considering that each pair of pulses is detected in the same basis, Bob will always be blinded by Eve for both pulses or neither pulses, resulting in the same factor 1/2 for both single and double-detection events

Table 4. The background noise is defined as the gain of the single (non-empty) and empty pulses, $Q_{(+)}$ and $Q_{(-)}$, respectively, where μ is the expected photon number of the source and Y_0.

2. The transmittance η_i of i photons' state at Bob's, that is, $\eta_{BTi} = 1 - \left(1 - \eta_{BT}\right)^i$ for $i = 0, 1, \ldots$, assuming independence among the i photons of the i photons' state;
3. The yield Y_i of the i photons' state is acquired from two sources, the background noise (Y_0) and the true signal. Presuming that the background counts are independent from the signal photon detection, Y_i is given by $Y_i = Y_0 + \eta_{BTi} - Y_0\eta_{BTi}$. However, assuming Y_0 is small (around 10^{-5}) and $\eta_{BT} \sim 10^{-3}$, the above equation can be reduced to $Y_i \sim Y_0 + \eta_{BTi}$.

The overall gain $Q_{(+)}$ is the summation of each Q_i contribution, thus: $Q_{(+)} = \sum_{i=1}^{\infty} Q_i = \sum_{i=1}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu}$, which leads to the relation $Y_0 + 1 - e^{-\mu\eta_{BT}}$. Finally, the quantum bit error rate (*QBER*) between Alice and Bob has been derived by Ma et al. [18] through the relation $QBER_{AB} = \frac{0.5Y_0 + e_d(1 - e^{-\mu\eta_{BT}})}{Y_0 + 1 - e^{-\mu\eta_{BT}}}$, where e_d is the error probability of the detector $\left(e_d \sim 10^{-2}\right)$.

With the aim to obtain the gain of double-detection events $Q_{(-,-)}$, $Q_{(\pm,\mp)}$, and $Q_{(+,+)}$, we consider that each gain has independence of any other, that is, $Q_{(-,-)} = Q_{(-)} \times Q_{(-)}$, $Q_{(+,-)} = Q_{(+)} \times Q_{(-)}$, $Q_{(+,-)} \sim Q_{(-,+)}$, and $Q_{(+,+)} = Q_{(+)} \times Q_{(+)}$. From the previous discussion, we know that the gain of the double-detection events decreases quadratically: $Q_{(+,+)} \sim Q_{(+)}^2$. In practical implementations of *QKD*, the single-matching events have the order of 10^{-5}, while the double-matching events reach the order of 10^{-10}.

5.2. Detecting the photon number splitting attack

In replacing T_{AB}, the photonic gain of the single-detection events or the double-detection events can be adjusted by Eve but not both at the same time. In contrast, Alice utilizes the

double-matching detection events ($2M$) and the (S-i) sifting instances which are consistent with the states she fixed, to verify corresponding photonic gains, *parallel* and *non-orthogonal*.

As mentioned before, the one-photon states are blocked by eavesdropper and she performs a channel substitution to adjust the transmittance of the channel, T_{AB}. Nevertheless, this activity produces error gains in the single- and double-detection events that Alice can verify.

The *QPEG* after Eve blocks the one-photon states and can be written as $\Delta Q = Q_1$ where Q_1 is the gain of the one-photon states and it must be computed for the single- and the double-detection events. The error gain is $\Delta Q_{(+,+)} = Q^2_{1_{(+)}} = Q^2_1$ and $\Delta Q_{(\pm,\mp)} = Q_1 \cdot Q_{(-)}$ for double-detection events and single-detection events, respectively, where $Q_{1_{(+)}} = (Y_0 + \eta - Y_0\eta)\mu e^{-\mu}$, $Q_{(-)} = e^{-\mu\eta} - Y_0$, η is the transmittance of the channel, and the detectors at Bob's side of the one-photon states and Y_0 is the background noise according to Ma et al. [18].

The eavesdropper must adjust the transmittance, T_{AB}, in order to remain hidden in the channel to achieve the two reference photonic gains, $Q_{(+,+)}$ and $Q_{(\pm,\mp)}$, for the double-detection events and single-detection events, respectively. Given $Q_{(+,+)} \neq Q_{(\pm,\mp)}$ Eve can adjust T_{AB} to Q^2_1 or $Q_1 \cdot Q_{(-)}$ but not both simultaneously. In other words, she is not able to fulfill the conditions $\Delta Q_{(+,+)} = 0$ and $\Delta Q_{(\pm,\mp)} = 0$; in this manner, the attack becomes detectable. If the eavesdropper adjusts T_{AB} to make it produce a photonic deviation in one or in both gains, she will introduce a detectable *QBER* to the system.

Consequently, Eve knows that she must be careful and makes no changes in T_{AB}; otherwise, she will be detected. Now, the *QBER* that Eve produces is $\frac{0.5Q_0+0.5^2Q_1+0.5^3Q_2+\ldots}{Q_0+Q_1+Q_2+\ldots}$ because the *QBER* of single-detection events is 0.5^2 as in *BB84*. In contrast, when no attack is produced the *QBER* of the system is given by $\frac{0.5Q_0+e_d(Q_1+Q_2+Q_3+\ldots)}{Q_0+Q_1+Q_2+\ldots}$ where e_d is the detection error according to Ma et al. [18].

Given that the probability of obtaining a (compatible) matching measurement from the *non-orthogonal* double-detection events is 0.5^2, we derived the error rate of the *non-orthogonal* double-detection events as $\frac{0.5(Q_0+Q_1)+0.5^2Q_2+0.5^3Q_3+\ldots}{Q_0+Q_1+Q_2+\ldots}$. The *QBER* from the multi-photonic *non-orthogonal* states decreases one-half for each copy of quantum states in Eve's memory. In contrast, no contribution is made by the multi-photonic *parallel* states to increase the *QBER* because Bob makes public the basis measurements used by him.

6. The *IRFS* attack

What should Alice and Bob expect from the nonappearance of the *IRFS* attack? For illustrative purposes, consider the situation where $\mu = 0.2$, $\eta_{BT} = 0.8$, which is the general efficiency among Alice and Bob and zero dark counts ($Y_0 = 0$). In such a case, the great majority of the total biqubits sent by Alice to Bob ends up in Bob's station as lost biqubits ($\sim 72.61\%$); single-detection events are $\sim 25.2\%$, and just $\sim 0.0219\%$ of the measurement cases are double-detection events. Despite the double-detection gain being very low, it ought not be viewed as

insignificant given that the amount of pulses sent by Alice is high ($10^{11} - 10^{13}$ [29]), and the transmission interim can be legitimately upgraded. However, for practical purposes, we will presume that the secret bits in the *nack state* protocol are delivered by single-detection events, and the key rate is at most the *BB84* key rate. Nevertheless, we assert that double-detection events can be utilized to identify the *IRFS* attack, so in this section, we defend the security of the protocol, in spite of Eve's endeavors to enhance her attack.

6.1. Detecting the *IRFS* attack with blinding pulses and quantum channel substitution

Within the sight of the *IRFS* attack with blinding pulses, Eve is amid the quantum channel utilizing an optical detection system comparable to Bob's station. Eve is challenged to reproduce gains of single- and double-detection events at Bob's side to pass unnoticed in the quantum channel. However, the gain of the single-detection events decreases directly with the channel efficiency, but the double-detection gain drops quadratically. In the next section we demonstrate that, for practical parameters of the quantum channel, the two gains cannot be adjusted by the eavesdropper at the same time. Eve cannot control the two gains because of the fact that:

1. the transmittance of the channel can be adjusted to a unique value by the eavesdropper either to adjust the single or the double-detection gain and
2. Eve's station receives Alice's optical pulses sequentially. In this manner, once a pulse is detected in the eavesdropper station, she is not able to know whether the next pulse will be likewise detected or lost. That is, Eve has no form to know when a single or a double-detection event will occur.

Eve still has the possibility to adjust the efficiency of the quantum channel to the gain of the double-detection events. Therefore, with the purpose of removing the excess of the single-detection gain, Eve could eliminate pulses in proportion to some probability (e.g., 0.5). However, in accordance with the second statement given previously in this section, the eavesdropper would lose double-detection pulses (a quarter in this example). Eve could be more selective discarding only single-detection events on which the detection occurred in the second pulse. By using this scheme, the double-detection gain is unaltered for Eve. However, given that the number of single detections inside the biqubit, first or second (see **Table 3**), is announced by Bob publicly, the presence of Eve becomes evident.

Both strategies could be combined by Eve to increase the efficiency of the channel to produce an overabundance of the double-detection gain, but it would also increase the single-detection gain. The issue for Eve is that once a strategy to remove pulses is chosen, it affects equally the single- and the double-detection gains. Such gains obey diverse rates: while the first decreases linearly, the second fluctuates quadratically with the transmittance of the channel. Moreover, at the receiver station, the single- and double-detection events are registered as haphazard interleaved events.

In the following sections, a convenient method to compute the photon gain deviation caused by the *IRFS* attack at a practical level is discussed.

6.2. Detecting the *IRFS* attack with quantum channel substitution

It is expected that the eavesdropper would endeavor to adjust both gains, from single- and double-detection events, applying a quantum channel substitution and tuning it to a specific transmittance. We define the quantum photon error gain (*QPEG* or simply ΔQ) as the deviation from the reference gain that is caused by Eve's apparatus at Bob's receiver station when she performs the *IRFS* attack. In ordinary conditions, it is ideally expected that $\Delta Q \sim 0$, for the single- and the double-detection events.

QPEG of double $(+,+)$-detection events is written as $\Delta Q_{(+,+)}$, while we denote the *QPEG* of single $(\pm, \mp)$-detection events as $\Delta Q_{(\pm,\mp)}$. $\Delta Q_{(+,+)}$ is computed as the difference $Q_{(+,+)_{AB}} - Q_{(+,+)_{EB}}$ where the symbol $(+,+)_{AB}$ defines the reference gain of the double-detection events and $(+,+)_{EB}$ denotes the gain of the double-detection events at Bob's side but in the presence of Eve. Similarly, $\Delta Q_{(\pm,\mp)}$ is computed as $Q_{(\pm,\mp)_{AB}} - Q_{(\pm,\mp)_{EB}}$, where we apply the sub-index of $(\pm, \mp)_{AB}$ and $(\pm, \mp)_{EB}$ with the same intention.

Using the relations of **Table 4**, the possibility of the eavesdropper to fulfill simultaneously the conditions $\Delta Q_{(+,+)} = 0$ and $\Delta Q_{(\pm,\mp)} = 0$ can be established. Allow Eve to adjust freely η_{BT} and η_{ET}. Thus, the eavesdropper's goal is to make $\Delta Q_{(+,+)_{AB}} = \Delta Q_{(+,+)_{EB}}$ and $\Delta Q_{(\pm,\mp)_{AB}} = \Delta Q_{(\pm,\mp)_{EB}}$. The following equation system is obtained:

$$2(e^{-\mu\eta_{BT}} - Y_0)(Y_0 + 1 - e^{-\mu\eta_{BT}}) = (e^{-\mu\eta_{ET}} - Y_0)(Y_0 + 1 - e^{-\mu\eta_{ET}}) \quad (1)$$

$$(Y_0 + 1 - e^{-\mu\eta_{BT}})^2 = \frac{1}{2}(Y_0 + 1 - e^{-\mu\eta_{ET}})^2 \quad (2)$$

Solving the system for η_{ET}, we get $\frac{\ln Y_0}{-\mu}$ and $\frac{\ln(1+Y_0)}{-\mu}$, which, in the practice, cannot be satisfied, given that the second relation yields η_{ET} as negative and the first relation cannot be fulfilled for typical parameters, for example, $Y_0 = 10^{-5}$, $\mu = 0.1$ produces $\eta_{ET} = 1.15$. Consider also the cases depicted in **Figure 6**.

6.3. The photon and the vacuum ratios

We will introduce a convenient method to detect the presence of the eavesdropper without requiring one to compute deviations from the reference gain, that is, $\Delta Q(+,+) = 0$ or $\Delta Q(\pm, \mp) = 0$. For this purpose, let us define the photon ratio R as the relation between the gains $\frac{Q_{EB}}{Q_{AB}}$ where the subscript EB denotes the presence of the eavesdropper and AB indicates its absence. For double-detection events, we represent R as $\frac{Q(+,+)_{EB}}{Q(+,+)_{AB}}$, while $\frac{Q(\pm,\mp)_{EB}}{Q(\pm,\mp)_{AB}}$ for single-detection events. In addition, we will define the vacuum ratio r as $\frac{e^{-\mu\eta_{ET}} - Y_0}{e^{-\mu\eta_{BT}} - Y_0}$.If the eavesdropper adjusts the channel to achieve $Q(+,+)_{AB} = Q(+,+)_{EB}$, then Eq. (2) is satisfied. We get that $R_{(\pm,\mp)} = \frac{r}{\sqrt{2}}$, but $r = \frac{e^{-\mu\eta_{ET}} - Y_0}{e^{-\mu\eta_{BT}} - Y_0}$ and $\eta_{ET} \geq \eta_{BT}$; thus, $r \leq 1$ and $R_{(\pm,\mp)} \leq \frac{1}{\sqrt{2}}$. To discard Eve's presence, it is not necessary to verify that $\Delta Q(\pm, \mp) = 0$, but it must be confirmed that $R_{(\pm,\mp)} > \frac{1}{\sqrt{2}}$.

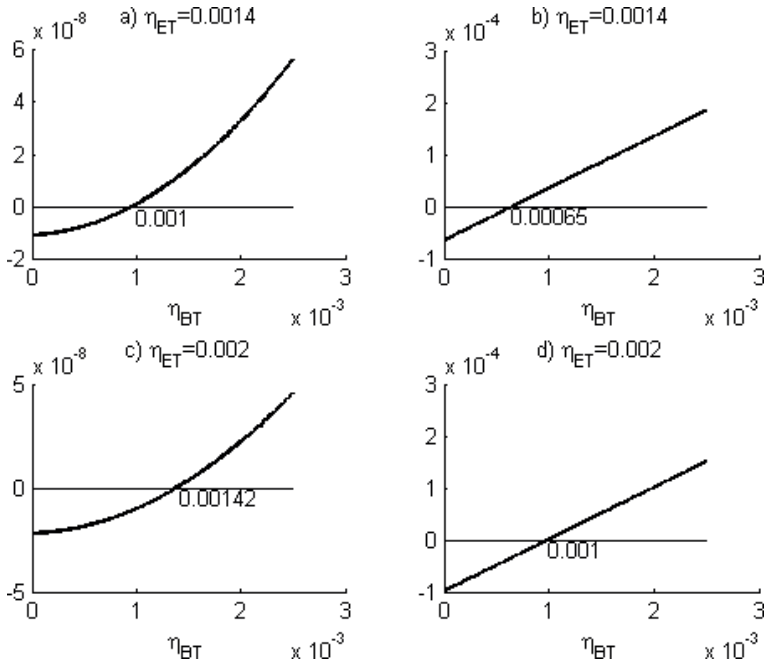

Figure 6. The deviation from the reference gain is shown on the *y*-axis. The upper and bottom left graphs represent double detections, while the right graphs correspond to single detections. Considering that $\eta_{BT} = 0.001$ and Eve uses $\eta_{ET} = 0.0014$, she accomplishes in (a), $\Delta Q_{(+,+)} = 0$, however, in (b), $\Delta Q_{(\pm,\mp)} \neq 0$. Conversely, if Eve adjusts $\eta_{ET} = 0.002$, she gets in (d)) $\Delta Q_{(\pm,\mp)} = 0$, but in (c), she provokes simultaneously that $\Delta Q_{(+,+)} \neq 0$.

Contrarily, if Eve modifies the channel to achieve $Q(\pm, \mp)_{AB} = Q(\pm, \mp)_{EB}$, we get that $R_{(+,+)} = \frac{2}{r^2}$. Since $r \leq 1$, we obtain that the *IRFS* attack causes $R_{(+,+)} \geq 2$. To make sure that the system is protected against the *IRFS* attack, it is not necessary to check $\Delta Q(+,+) = 0$ but it is enough verifying its equivalent $R_{(+,+)} < 2$.

6.4. The *QBER* of one-photon states

As quoted previously, in the *nack state* protocol, the great majority of the pulses sent by Alice to Bob behave as *BB84* signal pulses. Each time a compatible basis measurement is applied by Bob, the result, either from single detection or double detection, is useful as in *BB84*. Thus, for practical purposes, the *nack state* protocol has an efficiency comparable to the *BB84*. However, a partial reduction of the bit rate can be expected, as Alice reduces the optical pulse rate to avoid the eavesdropper to record double-detection events. In this way, Eve is detected if she stays waiting for double-detection events before she can forward them.

Given that it decreases quadratically, the rate of the double-detection event is small. Nevertheless, at the same time, it is extraordinary that the *QBER* of the double-matching detection events from *parallel* and *orthogonal* states also decreases quadratically. To see this, let us recall

http://dx.doi.org/10.5772/intechopen.75964

that in the *BB84* protocol, the probability to get the correct bit is $pc = (1 + V)/2$, and the probability to obtain an erroneous bit is $pe = (1 - V)/2$, where V is the visibility of the optical system. To calculate the *QBER* of the one-photon states, the relation $QBER = pe/(pe + pc)$ is applied [31].

Now, suppose that the two *parallel* states are sent by Alice $(|1_Z\rangle, |1_Z\rangle)$ to Bob who measures them using the Z basis. Those states are depicted in **Figure 7a**. The probability to get the two states $(|1_Z\rangle, |1_Z\rangle)$ is p_c^2, and the probability to get the opposite values $(|0_Z\rangle, |0_Z\rangle)$ is p_e^2, case II of **Figure 7a**. Since the measurement cases $(|0_Z\rangle, |1_Z\rangle)$ and $(|1_Z\rangle, |0_Z\rangle)$, Cases III and IV of **Figure 7a**, are always disposed because they are non-matching cases, the final probabilities are $pc_{parallel} = \frac{p_c^2}{p_c^2+p_e^2}$ and $pe_{parallel} = \frac{p_e^2}{p_c^2+p_e^2}$. The same reasoning can be applied to the *orthogonal* biqubits case as depicted in **Figure 7b**.

Those relations forward us to the *QBER* of the *parallel* and *orthogonal* states $QBER = \frac{(1-V)^2}{(1-V)^2+(1+V)^2}$. **Figure 8** gives an illustration of the *QBER* of one-photon states of such protocols. Considering the *QBER* of the *nack state* is lower than *BB84*, it is interesting to acknowledge that the double-

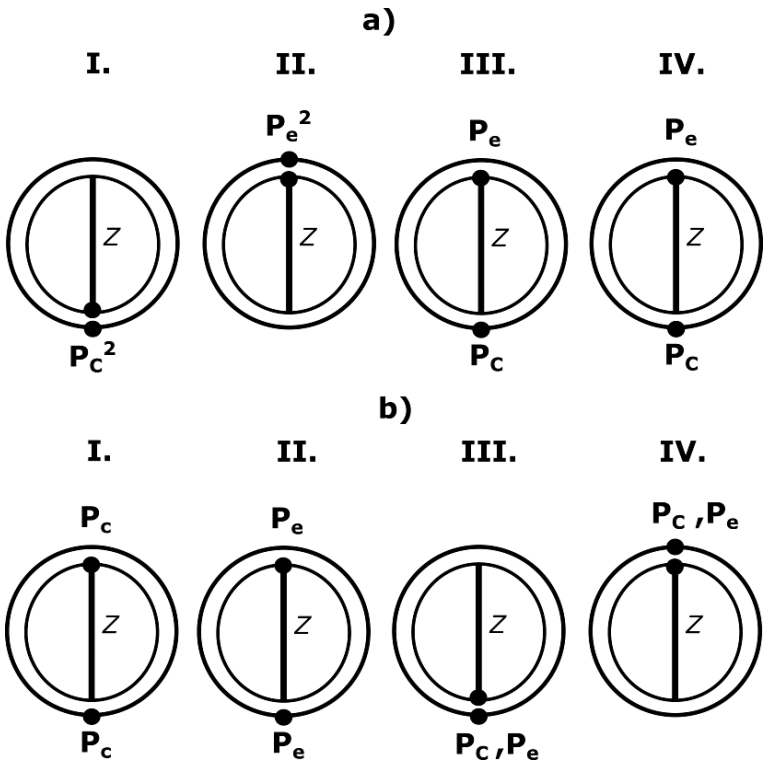

Figure 7. The *QBER* of *parallel* and *orthogonal* states: Cases III and IV of (a) and (b) can be discarded by Alice, so they do not produce errors.

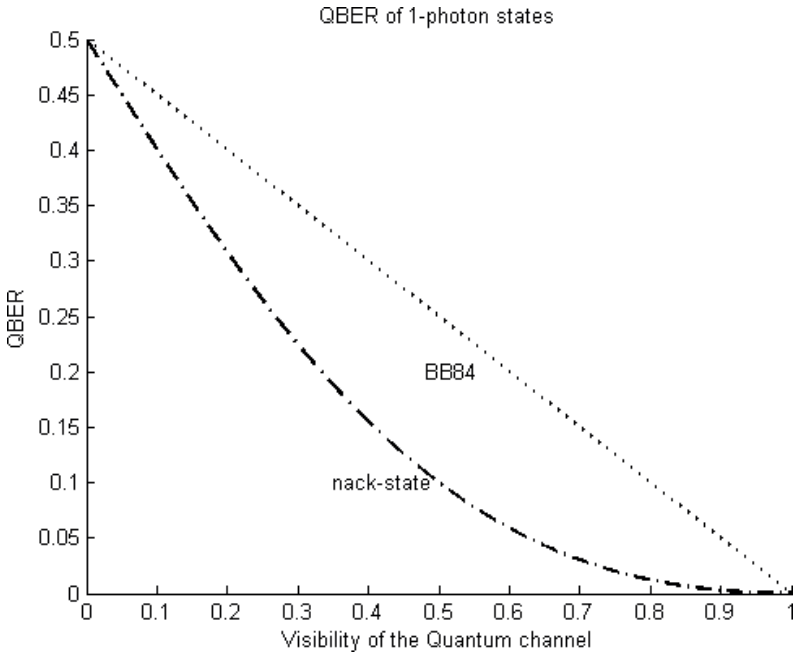

Figure 8. The *nack state* protocol uses pairs of *parallel* and *orthogonal* states. The *QBER* of *parallel* and *orthogonal* states is derived using the probabilities of two consecutive *BB84* measurements.

detection gain could be increased by future technologies. Even though there is not yet a formal derivation of the secret key rate for double-detection events, we can expect that the small *QBER* would lead to reaching longer *QKD* distances.

6.5. The non-structured *nack-state* protocol

In the argument of Point 2 of Section 6.1, it is implicit that Eve uses only a single station, but this is not a practical restriction. Eve could use two stations, one near to Alice to detect and one near to Bob to generate fake pulses. In the event that quantum channel utilizes optical fibers (the most widely recognized useful channel for ground-based *QKD*), everything required by Eve is a radio connection between her two stations to "catch up" with the quantum link. Even assuming a low source rate of 1 MHz, the time delay between pulses is only 1 microsecond, which can be easily compensated using a 600 m link (traveling in free space takes 2 microseconds; traveling in fiber takes 3 microseconds). Any practical *QKD* system will operate over distances greater than 600 m, making it entirely achievable for Eve to detect both pulses of a pair before transmitting her fake state to Bob using a second station.

A 100 km link in optical fiber would limit the source rate to 6 kHz, and much less if the fiber is not straight, which is almost always the case. To truly be secure the period between two pulses would have to be the full travel time of the pulse over the quantum channel. For 100 km, it

would be 500 microseconds, forcing a source rate of 2 kHz. Given the conservative fiber link loss of 0.2 dB/km the detection rate after 100 km (20 dB) would be less than 20/s, not counting detection efficiency. Shorter distances would be more favorable, but this implies the protocol is limited to short distances. There also is not any point in randomly adding delays as Eve would still be able to perfectly replicate the gains when the delay is insufficient and could choose to simply not intercept when the delay is too long, giving her partial information without any hint of her presence.

Unfortunately for Eve, Alice can apply a reduction in the optical pulse rate forcing Eve to introduce a delay in the arrival time of the pulses at Bob's station. As a matter of fact, Alice could adjust such delay sending slow pulses as a random burst. Furthermore, slowing pulses can enhance the double-detection rate at Bob's side by reducing after-pulsing errors.

However, there is no reason why each pair must be sent in sequence. We call this protocol the non-structured *nack-state*. If Alice were to transmit a burst of the first states of each pair, followed by a burst of the second states of each pair, she would create a separation between the pairs equal to the length of the bursts and she would not reduce the pulse rate. Consider a 100 km fiber optic link; it would be able to send the first states of each pair for 500 microseconds, followed by the second state of each pair for the next 500 microseconds, with Bob rechoosing the same basis for both 500 microsecond bursts. Since the 500 microsecond delay is at least the full travel time in the quantum channel, Eve would always be compelled to fake the first state of each pair before receiving the second. If there is no issue with this approach, the authors can use it to justify Point 2 of Section 6.1, which in turn justifies Point 1 of the same section.

6.6. Faking double-detection events

Another possibility for the eavesdropper is to fake double-detection events. After all, we may inquire why Eve cannot fake double-detection events as she stays covered up in the channel. First of all, let us recall that Alice knows which biqubits contain *parallel* or *orthogonal* states. Second, consider the cases portrayed in **Table 5**. Assume the $(|0_Z\rangle, |0_Z\rangle)$ biqubit has been sent to Bob by Alice. The first pulse reaches Eve's station, who measures it with the X (or Z) basis, but the second pulse arrives as a vacuum state either by the effect of the quantum channel, the detection system, or the photon source. Thus, Eve gets a single-detection event. In this moment, Eve determines to fake the second state, but she realizes that there are six potential outcomes to fake the $(|0_Z\rangle, |0_Z\rangle)$ biqubit; such cases are listed in **Table 5**. Additionally, one of those cases is erroneous because no *orthogonal* measurement can be derived from *parallel* states. In this example, $(|1_Z\rangle, |0_Z\rangle)$ cannot be obtained from $(|0_Z\rangle, |0_Z\rangle)$. Likewise, $(|0_Z\rangle, |0_Z\rangle)$ cannot be derived from $(|1_Z\rangle, |0_Z\rangle)$. Consequently, if Eve tries to fake a double-detection event, she will produce a bit error of $\frac{1}{6}$. In this situation, a bit error is produced when Alice expects a double non-matching event but Bob announces a double-matching event or vice versa.

According to Collins et al. [30], Bob's visibility of Alice's quantum state is computed as $V_{AB} = \frac{P(signal)}{P(total)}$ where $P(signal) = T_{AB} \times \eta \times V_{opt}$ and $P(total) = T_{AB} \times \eta + (1 - T_{AB} \times \eta) \times 2 \times Y_0$. Here, V_{opt} is the optical visibility with a perfect source and detectors; η is the probability

Alice's Biqubit	Eve's Basis	Eve's Detection	Forwarded States	Eve's Result
$(\|0_Z\rangle, \|0_Z\rangle)$	Z	$(-, \|0_Z\rangle)$	$(\|0_Z\rangle, \|0_Z\rangle)$	Hidden
			$(\|1_Z\rangle, \|0_Z\rangle)$	Detected
	X	$(-, \|0_X\rangle)$	$(\|0_X\rangle, \|0_X\rangle)$	Hidden
			$(\|1_X\rangle, \|0_X\rangle)$	Hidden
		$(-, \|1_X\rangle)$	$(\|0_X\rangle, \|1_X\rangle)$	Hidden
			$(\|1_X\rangle, \|1_X\rangle)$	Hidden
$(\|1_Z\rangle, \|0_Z\rangle)$	Z	$(-, \|0_Z\rangle)$	$(\|0_Z\rangle, \|0_Z\rangle)$	Detected
			$(\|1_Z\rangle, \|0_Z\rangle)$	Hidden
	X	$(-, \|0_X\rangle)$	$(\|0_X\rangle, \|0_X\rangle)$	Hidden
			$(\|1_X\rangle, \|0_X\rangle)$	Hidden
		$(-, \|1_X\rangle)$	$(\|0_X\rangle, \|1_X\rangle)$	Hidden
			$(\|1_X\rangle, \|1_X\rangle)$	Hidden

However, she can use six possible states, but one of them is erroneous, so she introduces an error probability of $\frac{1}{6}$. Here, the six choices for $(|0_Z\rangle, |0_Z\rangle)$ and $(|1_Z\rangle, |0_Z\rangle)$ biqubits are shown

Table 5. As soon as Eve detects the first state of a biqubit, she tries to fake the second state.

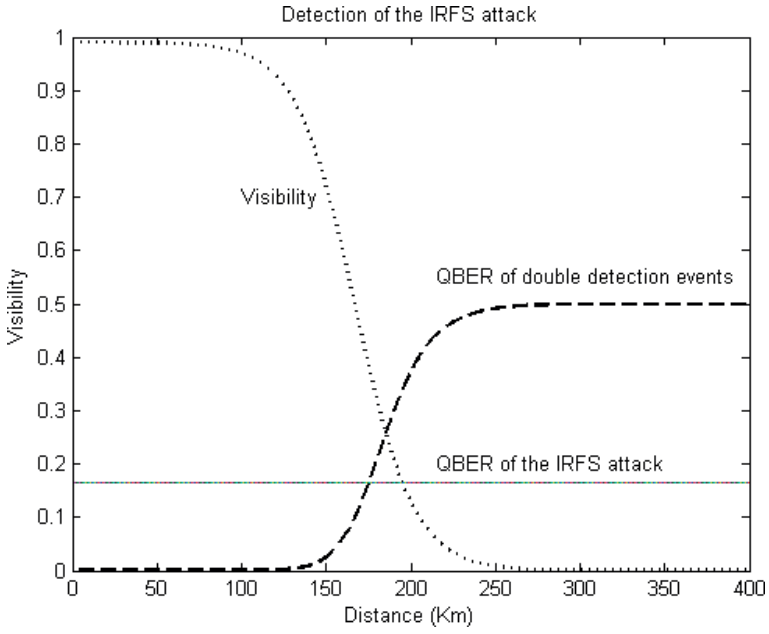

Figure 9. The error rate of double-detection events caused by the *IRFS* attack is $\frac{1}{6}$. When it is compared to the *QBER* of the quantum channel, the maximum secure distance to detect the *IRFS* attack is 176 km. In the presence of the *IRFS* attack, perfect visibility and zero dark counts are assumed in the link between Alice and Eve and from her to Bob.

of detecting the photon when it arrives; T_{AB} is the transmittance between Alice and Bob; and Y_0 is the background noise. On practical experimental parameters: $\alpha = 0.25$ dB· km^{-1}, $\eta = 0.3$, $Y_0 = 10^{-4}$, and $V_{opt} = 0.99$. **Figure 9** shows the visibility as a function of the distance.

On the other hand, the *QBER* in *BB84* can be computed as $QBER = \frac{pe}{pe+pc}$, where *pc* (*pe*) is the probability to get, correctly or erroneously, the quantum bit sent by Alice, respectively. If we write such probabilities as a function of the optical visibility V, we have $pc = (1 + V)/2$ and $pe = (1 - V)/2$.

Therefore, $pc = \frac{p_c^2}{p_c^2+p_e^2}$ and $pe = \frac{p_e^2}{p_c^2+p_e^2}$, and we derived the *QBER* of the *parallel* and *orthogonal* states as $QBER = \frac{(1-V)^2}{(1-V)^2+(1+V)^2}$.

If *QBER* of double-detection events produced by the quantum channel is compared against the $\frac{1}{6}$ error rate caused by the eavesdropper, we can find that the maximum secure distance for detecting the *IRFS* attack when the eavesdropper fakes double-detection events is 176 km, which is within the range of the *BB84* key rate, as it appears in **Figure 9**.

7. Conclusions

In the quantum flows approach, the transmitter interleaves pairs of quantum states, *parallel* and *orthogonal* (*non-orthogonal*), while the receiver applies active basis selection to perform state measurement. The *QKD* protocols based on quantum flows uses the same optical hardware of the *BB84* protocol, and they can be implemented in most *QKD* systems as a software module application.

The *ack-QKD* protocol can be useful to detect the *PNS* attack. If the eavesdropper adjusts the transmittance T_{AB} of the channel it produces a deviation in one or in both photonic gains; thus, she will introduce a detectable *QBER* to the system.

On the other side the intercept resend with faked (blinding) states (*IRFS*) attack is detected by the *nack-state* protocol using the gain of single- and double-detection events where the *QBER* of double-detection events of the quantum channel is compared against the $\frac{1}{6}$ error rate caused by the eavesdropper, so the maximum secure distance results in 176 km.

Although double-detection events represent a small fraction of the total detection events, they are useful to detect the *IRFS* attack. In addition, the smaller *QBER* can be useful in future implementations to distill secret bits at longer distances.

Acknowledgements

We would like to mention that a major portion of this chapter has been borrowed from our previous publications: "Quantum Flows for Secret Key Distribution in the Presence of the

Photon Number Splitting Attack" [5] and "Quantum Key Distribution in the Presence of the Intercept-Resend with Faked States Attack" [6].

Author details

Luis A. Lizama-Pérez[1]*, J. Mauricio López[2] and Eduardo de Carlos Lopez[3]

*Address all correspondence to: luislizama@upp.edu.mx

1 Universidad Politécnica de Pachuca, Ex-Hacienda de Santa Bárbara, Municipio de Zempoala, Hidalgo, México

2 Cinvestav Querétaro, Santiago de Querétaro, Querétaro, México

3 Time and Frequency Laboratory, Centro Nacional De Metrología, Santiago de Querétaro, Querétaro, México

References

[1] Bennett CH. Quantum cryptography public key distribution and coin tossing. In: Proceedings of the 1984 International Conference on Computer System and Signal Processing; 1984; Bangalore. pp. 10–19

[2] Van Assche G. Quantum Cryptography and Secret-Key Distillation. Cambridge: Cambridge University Press; 2006

[3] Hughes R, Nordholt J, Rarity J. Summary of implementation schemes for quantum key distribution and quantum cryptography quantum information science and technology roadmap. Available online: http://qist.lanl.gov/pdfs/6.5-continuous.pdf [Accessed on 19 December, 2016]

[4] Lizama L, López JM, De Carlos E, Venegas-Andraca SE. Enhancing quantum key distribution (QKD) to address quantum hacking. Procedia Technology. 2012;**3**:80-88

[5] Lizama-Pérez LA, López JM, De Carlos-López E, Venegas-Andraca SE. Quantum flows for secret key distribution in the presence of the photon number splitting attack. Entropy. 2014;**16**:3121-3135

[6] Lizama-Pérez LA, López JM, De Carlos-López E. Quantum key distribution in the presence of the intercept-resend with faked states attack. Entropy. 2016;**19**

[7] Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. Journal of Cryptology. 1992;**5**:3-28

[8] Fung CF, Qi B, Tamaki K, Lo H. Phase-remapping attack in practical quantum-key-distribution systems. Physical Review A. 2007;**75**:032314

[9] Xu F, Qi B, Lo H. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. New Journal of Physics. 2010;**12**:113026

[10] Makarov V, Hjelme DR. Faked states attack on quantum cryptosystems. Journal of Modern Optics. 2005;**52**:691-705

[11] Makarov V, Anisimov A, Skaar J. Effects of detector efficiency mismatch on security of quantum cryptosystems. Physical Review A. 2006;**74**:022313

[12] Makarov V, Skaar J. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. Quantum Information and Computation. 2008;**8**: 622-635

[13] Qi B, Fung CF, Lo H, Ma X. Time-shift attack in practical quantum cryptosystems; 2005. arXiv:quant-ph/0512080

[14] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics. 2010;**4**: 686-689

[15] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C, Makarov V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Communications. 2011;**2**:349

[16] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt C, Makarov V, Leuchs G. After-gate attack on a quantum cryptosystem. New Journal of Physics. 2011;**13**:013043

[17] Weier H, Krauss H, Rau M, Fuerst M, Nauerth S, Weinfurter H. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. New Journal of Physics. 2011;**13**:073024

[18] Ma X, Qi B, Zhao Y, Lo H. Practical decoy state for quantum key distribution. Physical Review A. 2005;**72**:012326

[19] Hughes R, Nordholt J. Refining quantum cryptography. Science. 2011;**333**:1584-1586

[20] Lo H, Curty M, Qi B. Measurement-device-independent quantum key distribution. Physical Review Letters. 2012;**108**:130503

[21] Lunghi et al. Free-running single-photon detection based on a negative feedback InGaAs APD. Journal of Modern Optics. 2012;**59**:1481-1488

[22] Gottesman D et al. Proof of security of quantum key distribution with two-way classical communication. IEEE Transactions on Information Theory. 2003;**49**:457-475

[23] Shor P et al. Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters. 2000;**85**:441

[24] Scarani V et al. The security of practical quantum key distribution. Reviews of Modern Physics. 2009;**81**:1301

[25] Scarani V et al. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. Physical Review Letters. 2004;**92**:057901

[26] Takesue H et al. Differential phase shift quantum key distribution experiment over 105 km fiber. New Journal of Physics. 2005;**7**:232

[27] Stucki D et al. Coherent one-way quantum key distribution. Proceedings of SPIE. 2007; **6583**

[28] Sun S, Jiang M, Ma X, Li C, Liang L. Hacking on decoy-state quantum key distribution system with partial phase randomization. Scientific Reports. 2014;**4**:013043

[29] Song T, Qin S, Wen Q, Wang Y, Jia H. Finite-key security analyses on passive decoy-state QKD protocols with different unstable sources. Scientific Reports. 2015;**5**:735-753

[30] Collins D, Gisin N, De Riedmatten H. Quantum relays for long distance quantum cryptography. Journal of Modern Optics. 2005;**52**:735-753

[31] Jeong Y, Kim Y-S, Kim Y-H. Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols. Laser Physics. 2011;**21**:1438-1442